BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 15 845.6

Anmeldetag: 8. April 2003

Anmelder/Inhaber: Wolfgang R i c h t e r, Germering/DE

Bezeichnung: System, Systemkomponenten und Verfahren zur Abwicklung eines hermetisch validierbaren Datentransfers

IPC: H 04 B, H 04 L und B 60 R

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 4. Dezember 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Letang

A 9161
03/00
EDV-L

SYSTEM, SYSTEMKOMPONENTEN UND VERFAHREN ZUR ABWICKLUNG EINES HERMETISCH VALIDIERBAREN DATENTRANSFERS

Gebiet der Erfindung

Die Erfindung bezieht sich auf ein System, dessen Systemkomponenten sowie ein Verfahren zur Abwicklung eines Datentransfers in einer hinsichtlich der Validität eines Senders und/oder Empfängers geprüften Weise. Weiterhin befasst sich die Erfindung mit einem quasi unidirektionalen Dialogsystem zur Abwicklung einer Datenübertragung, insbesondere über den menschlichen Körper oder zumindest den Nah-Umgebungsbereich eines Anwenders.

Hintergrund der Erfindung

Bei funkbasierten Datenübertragungssystemen besteht das Problem, dass aufgrund der Ausbreitung der Funkwellen Unbefugte mit geeigneten Empfängern Daten aufzeichnen und missbrauchen können (s. Abb.1).

Insbesondere Systeme unter Einschluss elektromagnetischer Transponder lassen sich missbrauchen, auch wenn der Transponder weit von einem, diesen erkennenden Lesegerät entfernt ist. Dazu wird der Transponder zum Senden angeregt, und die erspähten Daten per Funk zu einem, an das Lesegerät angenäherten „Transpondersimulator" übermittelt, der dem Lesegerät vorgaukelt, der echte Transponder befände sich in der Nähe. Auf diese Weise wird es möglich Datensequenzen zur unzulässigen Zugangs- oder Leistungsverschaffung zu gewinnen. Das Prinzip einer solchen Reichweitenüberbrückung ist in Abb. 2 veranschaulicht.

Um diese Probleme zu vermeiden wurden sog. Challenge/Response-Lösungen entwickelt. Dabei werden zwischen einem Datengeber und einem Reaktionsgerät bidirektional Schlüsselwörter ausgetauscht. Neben einem aufwendigen Verfahren (Protokoll), was dieses ermöglicht, müssen sowohl Datengeber als auch Reaktionsgerät mit Sende- und Empfangseinrichtungen versehen sein und mit einer Steuerung wechselseitig betrieben werden. (s. Abb.3).

Wurde die Datenübertragung früher mit einem Knopfdruck (z.B. beim Funkautoschlüssel) eingeleitet, zeigt die Technik heute sog. Keyless-Access-Systeme, wo es genügt, mit einem Sendeempfänger in den Funkbereich eines Reaktionsgerätes zu treten. Doch damit tritt wiederum die Problematik der Reichweitenüberbrückung auf.

Für Challenge/Response-Systeme ergibt sich außerdem das Problem, dass ein, von einem Störsender ausgestrahlter starker Träger bei gleicher Frequenz das System daran hindern kann, Daten zu übertragen. Dieser Umstand ermöglicht es, missbräuchlich einen benutzerseitig angestrebten Türschließvorgang zu verhindern, so dass sich ein Besitzer eines Kraftfahrzeuges von diesem entfernt in dem Glauben, es sei verschlossen, weil er sich entweder aus dem Bereich der Keyless-Access-Erfassung entfernte oder einen Schließknopf seiner KFZ-Türfernbedienung betätigte. Ein mit einem geeigneten Handsender ausgestatteter Dieb, der einen Dauerträger aussendet, kann den Schließvorgang aus einiger Entfernung verhindern um anschließend Gegenstände aus dem Fahrzeug entwenden. Der geschädigte Besitzer kann gegenüber seiner Versicherung nicht nachweisen, dass das Fahrzeug verschlossen war. Als besonderes Problem könnte sich zudem herausstellen, dass anderweitige elektronische Systeme, ein

Benutzer oder auch unbeteiligte Personen durch die ständige Funkwellenbelastung gesundheitlich beeinträchtigt werden.

Um den Aufwand zu reduzieren und den Komfort einer fernbedienten Datenübertragung zu erhöhen, stellt die Technik Lösungen bereit, die Daten über den menschlichen Körper an einen berührungs- oder annäherungsempfindlichen Empfänger übermitteln. Damit sichergestellt ist, dass sich ein geeigneter Signalgeber zum Zeitpunkt der Datenübertragung in der Nähe des Empfängers befindet, wird eine Zeitmarke zusammen mit einer verschlüsselten Identifizierungsnummer übermittelt. Der Empfänger muss somit zeitsynchron mit dem Geber sein um eine unidirektionale Datenübertragung zu ermöglichen und sicherzustellen, dass der Code nicht in der Vergangenheit illegal kopiert und zu einem späteren Zeitpunkt beim Empfänger angewendet wurde (Timestamp). Der Vorteil der sicheren unidirektionalen Datenübertragung bringt hier das Problem der Synchronisierung und dem damit verbundenen Aufwand mit sich.

Aufgabe der Erfindung

Der Erfindung liegt die Aufgabe zugrunde, ein System, Systemkomponenten desselben und ein Verfahren zur Abwicklung eines, sich durch eine hohe Manipulationssicherheit auszeichnenden, Datentransfers zu schaffen.

Erfindungsgemäße Lösung

Der Erfindung liegt der Ansatz zugrunde, einen Datentransfer zwischen einem Mastersystem und einem Slavesystem in einer Weise abzuwickeln, die es ermöglicht, im Bereich des Mastersystems Informationen über das Slavesystem anhand der Signalaufnahmeeigenschaften desselben zu gewinnen.

Insbesondere zeigt die Erfindung eine Lösung auf, bei welcher ein Datentransfer zwischen dem Mastersystem und dem Slavesystem auf kapazitivem Wege erfolgt, wobei die Eingangsimpedanz des Slavesystems nach Maßgabe eines definierten Datenmusters moduliert wird und dieses Datenmuster im Bereich des Mastersystems während der Signalaussendung erkannt wird.

Dadurch wird es auf vorteilhafte Weise möglich, Informationen insbesondere in Form einer Schlüsseldatensequenz in einer quasi-hermetisch abgeschirmten Weise an ein Master- oder Sendesystem zurückzuführen und diese Schlüsseldatensequenz einer für den weiteren Datentransfer oder Datenaustausch maßgeblichen Signalgenerierung und/oder Signalvalidierung zugrundezulegen.

Unter dem Begriff Mastersystem ist im Kontext ein System zu verstehen, das in der Lage ist, eine, an einen Adressaten gerichtete Signalsequenz abzugeben. Unter dem Begriff Mastersystem ist im Kontext ein System zu verstehen, das in der Lage ist, ein seitens des Mastersystems bereitgestellte Datensequenz zu erfassen. Es kann ausreichend sein, das Master- oder das Slavesystem mit einer hinsichtlich seiner Eingangsimpedanz modulierbaren Empfangseinrichtung auszustatten. In Abstimmung auf den jeweiligen Anwendungsfall ist es möglich, schaltungstechnisch oder hinsichtlich der Datenverarbeitung aufwendigere Schaltungsstrukturen in den Bereich des Master- oder Slavesystems zu verlagern.

Im Hinblick auf die konkrete Abwicklung des Datentransfers wird die eingangs angegebene Aufgabe gelöst durch ein Verfahren zur Abwicklung eines Datentransfers zwischen einem Mastersystem (Geber) und einem Slavesystem (Empfänger) bei welchem seitens des Mastersystems ein Signalereignis in einen Empfangsbereich des Slavesystems hinein abgegeben wird und

die Empfangsaufnahmeeigenschaften des Slavseystems definiert moduliert und
seitens des Mastersystems erkannt und ausgewertet werden.

Der Datentransfer wird vorzugsweise auf Grundlage kapazitiver Wechselwirkungseffekte abgewickelt.

Vorzugsweise wird seitens des Mastersystems eine Pilotsequenz emittiert und während des Eingangs der Pilotsequenz die Eingangsimpedanz des Slavesystems nach Maßgabe eines Datenmusters moduliert.

Seitens des Mastersystems wird vorzugsweise die modulierte Änderung der Eingangsimpedanz des Slavesystems erfasst.

Aus dem seitens des Mastersystems erfassten Modulationsmuster der Eingangsimpedanz des Slavesystems wird in vorteilhafter Weise ein Datensatz generiert und dieser Datensatz maßgeblich für den Informationsinhalt oder für die Zulässigkeit einer Fortsetzung des Datentransfer von dem Mastersystem zu dem Slavesystem berücksichtigt.

Im Bereich des Mastersystems werden in vorteilhafter Weise aus den, aus dem Aufnahmeverhalten des Slavesystems gewonnenen Signalen Daten gewonnen, auf deren Grundlage eine Verschlüsselung der seitens des Slavesystems weiter ausgesendeten Daten erfolgt.

Im Bereich des Slavesystems kann in vorteilhafter Weise bei der Generierung des für die Modulation der Eingangsimpedanz relevante Datenmusters ein Zeitwert berücksichtigt werden.

Vorzugsweise werden im Bereich des Slavesystems für die Modulation der Eingangsimpedanz Informationsinhalte der seitens des Mastersystems generierten Signale berücksichtigt.

Die Modulation der Eingangsimpedanz des Slavesystems erfolgt vorzugsweise unter Rückgriffnahme auf eine Verschlüsselungsprozedur.

Die seitens des Slavesystems zur Bereitstellung der für die Modulation der Eingangsimpedanz maßgeblichen Datenmuster beigezogene Verschlüsselungsprozedur, kann in vorteilhafter Weise auf Grundlage von Informationsinhalten der seitens des Mastersystem ausgegebenen Signalsequenz konfiguriert oder abgestimmt werden.

In vorteilhafter Weise erfolgt im Rahmen der Dialogaufnahme eine Kongruenzanalyse zunächst auf Grundlage eines niedrigen Verschlüsselungsniveaus, wobei das Verschlüsselungsniveau anschließend angehoben wird.

Die für das angehobene Verschlüsselungsniveau maßgeblichen Informationsinhalte können zumindest zunächst auf niedrigeren Verschlüsselungsniveau transportiert werden.

Über das Mastersystem kann in vorteilhafter Weise eine, als Autorisierungskennung gewertete Signalsequenz je nach Anwendungsfall permanent, gepulst oder selektiv abgegeben werden.

Es ist möglich, das Mastersystem so auszugestalten, dass dieses eine Konfigurationsänderung des Mastersystems über die durch Impedanzmodulation gewonnenen Signale ermöglicht.

Der Datentransfer zwischen dem Mastersystem und dem Slavesystem kann in vorteilhafter Weise zur Abwicklung eines Zahl, Buchungs-, Wertstellungs- oder Zugangsnachweisvorganges herangezogen werden.

Der Datentransfer zwischen dem Mastersystem und dem Slavesystem kann auch zur Abwicklung eines Vorganges zur Änderung des Verriegelungszustandes eines Kraftfahrzeuges herangezogen werden.

Der Datentransfer zwischen dem Mastersystem und dem Slavesystem kann in weiterhin vorteilhafter Weise auch zur Funktionsfreigabe von Gerätschaften herangezogen wird.

Gemäß einem besonderen Aspekt der vorliegenden Erfindung kann der der Datentransfer zwischen dem Mastersystem und dem Slavesystem zur Durchführung einer Präsenzanalyse herangezogen werden, zur Feststellung des Ausstattungsumfanges oder des Zu- oder Abganges von selbstidentifizierenden Artikeln.

Die Erfindung bezieht sich auch auf ein System zur Abwicklung eines Datentransfers mit einer einem Mastersystemkomponente (Geber) und einer Slavesystemkomponente (Empfänger), wobei die Mastersystemkomponente derart ausgebildet ist, dass diese geeignet ist, ein Signalereignis in einen Empfangsbereich der Slavesystemkomponente hinein abzugeben, und die Slavesystemkomponente derart ausgebildet ist, dass diese es ermöglicht, die Empfangsaufnahmeeigenschaften derselben definiert zu modulieren, wobei im Bereich der Mastersystemkomponente Vorkehrungen getroffen sind, die Änderungen der Empfangseigenschaften der Slavesystemkomponente zu Erfassen und basierend auf dieser Erfassung den weiteren Datentransfer zu bestimmen.

Weiterhin beinhaltet die Erfindung auch eine Mastersystemkomponente für ein vorstehend angegebenes System, wobei diese eine Signalausgabeeinrichtung aufweist die als Flächenelektrode ausgebildet ist.

Diese Mastersystemkomponente umfasst vorzugsweise eine elektronische Signalverarbeitungseinrichtung, wobei die Signalverarbeitungseinrichtung vorzugsweise Zugriff zu einer Schlüsseldatenspeichereinrichtung hat.

Die Mastersystemkomponente kann in vorteilhafter Weise in einem scheckkartenförmigen Grundkörper aufgenommen sein.

Die Mastersystemkomponente kann Teil eines Fahrzeugschlüsselsystems bilden.

Die Erfindung richtet sich auch auf eine Slavesystemkomponente für ein System der oben genannten Art, wobei diese eine Empfangseinrichtung aufweist, zum Empfang von Eingangsereignissen auf Grundlage kapazitiver Wechselwirkungseffekte.

Die Slavesystemkomponente umfasst in vorteilhafter Weise eine Empfangseinrichtung die im Bereich eines Kassensystems, eines Personendurchgangsbereiches, eines Verkaufssystems oder einer Gerätschaft, z.B zur Freischaltung derselben angeordnet ist.

Die Slavesystemkomponente kann auch Teil eines Fahrzeugtürverriegelungssystems bilden.

Die Erfindung richtet sich auch auf ein Verfahren zur Änderung des Verriegelungszustandes eines Kraftfahrzeuges unter Abwicklung eines Datentransfers zwischen einem Mastersystem (Geber/Schlüssel) und einem Slavesystem (Empfänger/fahrzeugseitige Schaltungskomponente) bei welchem seitens des Mastersystems ein Signalereignis in einen Empfangsbereich des Slavesystems hinein abgegeben wird und die Empfangsaufnahmeeigenschaften des Slavseystems definiert moduliert und seitens des Mastersystems erkannt und ausgewertet werden.

Die Aufgabenverteilung oder Zuordnung des Mastersystems und des Slavesystems kann auch invertiert werden. Die Erfindung beeinhaltet damit auch ein Verfahren zur Änderung des Verriegelungszustandes eines Kraftfahrzeuges unter Abwicklung eines Datentransfers zwischen einem Mastersystem (Schlüsseleinrichtung) und einem Slavesystem (fahrzeugseitige Schaltungskomponente) bei welchem seitens des Slavesystems ein Signalereignis in einen Empfangsbereich des Mastersystems hinein abgegeben wird und die Empfangsaufnahmeeigenschaften des Mastersystems definiert moduliert und seitens des Slavesystems erkannt und ausgewertet werden

Der Datentransfer wird in vorteilhafter Weise auf Grundlage kapazitiver Wechselwirkungseffekte abgewickelt.

Weitere Einzelheiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung in Verbindung mit der Zeichnung. Es zeigt:

Abbildung 1 ein an sich bekanntes, einen Sender und einen Empfänger umfassendes Datenübertragungssystem , sowie ein beigestelltes Mithörsystem das einen unzulässigen Informationsabgriff ermöglicht;

Abbildung 2 ein an sich bekanntes elektromagnetisches Transpondersystem bei welchem ein Datentransfer zwischen dem Transponder und einem Lesegerät durch missbräuchliche Zwischenschaltung eines Schnüffelsystems bewerkstelligt ist;

Abbildung 3 eine Schemadarstellung zur Erläuterung eines Challenge/Response-Systems;

Abbildung 4 eine Schemadarstellung zur Erläuterung eines erfindungsgemäßen Systems zur Abwicklung einer hermetischen Signalrückführung durch Modulation der Empfangsimpedanz im Bereich des Empfängers;

Abbildung 5 eine Schemadarstellung zur vertieften Erläuterung des Systems nach Abbildung 4;

Abbildung 6 ein Diagramm zur Erläuterung des Aktivitätsablauf im im Bereich des Mastersystems (Geber) und dem Slavesystem (Empfänger).

Nachfolgend wird ein Verfahren vorgestellt, welches auf einfache Weise ein Dialogsystem realisiert, welches o.g. Probleme lösen kann. Dabei handelt es sich um eine kapazitive Übertragung von Daten, vorzugsweise über die Haut eines Benutzers. Da es sich hierbei prinzipiell um einen Wechselstromkreis handelt, kann eine Änderung der (z.B. ohmschen) Belastung der Empfängereingangsstufe senderseitig festgestellt werden. Diese Änderung kann in einem bestimmbaren Rhythmus erfolgen (sog. Belastungstelegramm BT s. Abb. 4).

Der Geber erzeugt zunächst einen kurzen (z.B. 1ms) Pilotton in unregelmäßigen Abständen wiederkehrend (repetierend) , z.B. 5 mal pro Sekunde. Bei Annäherung an die kapazitive Koppelstelle wird diese Frequenz vom Empfänger erkannt, der daraufhin sofort ein Belastungstelegramm (BT) erzeugt. Daran kann der Geber (Sender) „erkennen":

1. das er sich in der Nähe eines Empfängers befindet
2. um welchen Empfänger es sich handelt, wenn das BT eine Kennung enthält

3. auf welche Weise (Frequenz, Code, Schlüssel etc.) bestimmte Daten übertragen werden sollen
4. ob die Übertragung gestört wird, BT aufgrund eines Störträgers nicht korrekt lesbar

Ein „Mithörer" würde lediglich die Pilottöne detektieren können, da er zum Geber hin einen eigenen Belastungskreis bildet (Nicht jedoch zum Empfänger). An vom Empfänger entfernter Stelle könnten ohnehin lediglich die repetierenden Pilottöne „abgehört" werden, aufgrund des fehlenden Belastungstelegramms „erkennt" der Geber, das er sich nicht in Empfängernähe befindet und fährt fort, den Pilotton zyklisch auszugeben.

Der Empfänger ändert bei jedem Pilotton sein Belastungstelegramm. Einem Störträger „erkennt" er an der Überlänge (Dauerträger). Würde die Störung zyklisch erfolgen, wie die Pilottöne, so könnte aufgrund der unregelmäßigen Ausgabe der „echten" Pilottöne immer der eine oder andere „durchschlüpfen". Eine erkannte Störung kann einen Alarm auslösen oder z.B. eine Schließung einleiten oder anderweitig signalisiert werden. Da auf einen Pilotton vom Geber eine, durch das Belastungstelegramm verschlüsselte ID-Nummer ausgegeben werden muss, kann der Empfänger das Ausbleiben einer solchen ebenfalls feststellen.

Funktionsprinzip

Ein Oszillator (der auch als VCO ausgeführt sein kann) erzeugt die Übertragungsgrundfrequenz (typisch einige 100kHz). Eine Steuerung sorgt dafür, dass über einen Mischer (ASK/FSK o.ä.) zunächst die Pilottöne selektiv, oder zyklisch ggf. in unregelmäßigen Abständen ausgegeben werden. Bei Annäherung an einen Empfänger erzeugt dieser ein Belastungstelegramm (z.B.

durch Kurzschluß von Rb), was alternierende Spannungsabfälle am Widerstand Rx des Gebers zur Folge hat. Diese können z.B. über einen Differenzverstärker der Steuerung zugeführt werden. Diese dekodiert das Belastungstelegramm und verschlüsselt den zu übertragenden Code des Gebers entsprechend. Das Resultat wird wiederum über den Mischer ausgegeben, vom Empfänger verstärkt, dekodiert und einer Codeauswertung zugeführt. Beim Empfänger können Bauteile oder Komponenten in einen stromsparenden Zustand verbleiben, bis ein Pilotton empfangen wurde. Damit ist auf einfache Weise und mit geringem Aufwand ein komfortables und sicheres Dialogsystem mit vielen Vorteilen realisierbar (s. Abb. 5). Die Belastung des Wechselstromkreises kann durch das Ein- bzw. Ausschalten eines ohmschen Widerstands und/oder einer Kapazität und/oder einer Induktivität erfolgen. Der Schaltvorgang selbst kann durch einen Transistor, FET, CMOS-Schalter etc erfolgen; auch ein Optokoppler kann verwendet werden.

Eine erste bevorzugte Ausführung

Überall, wo eine sichere Identifikation innerhalb einer Handlung stattfinden soll (handlungsintegrierte Identifikation), können einer oder mehrere Codegeber bei einem Benutzer in Körpernähe untergebracht sein. Dies kann auf vielfältige Weise geschehen, z.B. können Chipkarten oder Schlüsselanhänger, Schmuck- oder Kleidungsstücke oder andere mitgeführte Gegenstände (Geldbörsen, Brieftaschen) Geber enthalten. Bei Annäherung eines Benutzers z.B. mit dessen Hand an einen Empfänger findet der quasi bidirektionale Dialog statt, weil ein Wechselstromkreis mit kapazitiven Koppelflächen entsteht. Nach der Übertragung identifizierender Daten kann der Empfänger bei Übereinstimmung dieser ein Signal ausgeben, welches z.B. eine elektromechanische Verriegelungseinrichtung zum Öffnen eines (Tür-) Verschlusses

bewirkt. Während die zu identifizierende Handlung erfolgt, wird im Rhythmus der Pilottöne ständig ein neuer Dialog mit unterschiedlichen Belastungstelegrammen geführt Eine Entfernung vom Empfänger veranlasst diesen, automatisch einen Schließimpuls auszugeben, der intern und extern verwendet werden kann. Keyless Access-Systeme erhalten damit eine neue Qualität, weil die kapazitive Methode zwischen zwei sich annähernden Flächen arbeitet und keinen (abhörbaren) Funkbereich benötigt. Außerdem gilt die Faustregel, dass wenn ein Geber ein Belastungstelegramm erkennen und dekodieren kann, die Übertragungsqualität (Quality of Service) der kapazitiven Koppelfläche für eine sichere geberseitige Datenübertragung ausreichend ist. Diesen Vorgang wollen wir „sensitive Intelligenz" nennen. Auf dieses Basis kann eine handlungsintegrierte Identifikation neu definiert werden:

1. Absicht eines, mit mindestens einem Codegeber ausgestatteten Benutzers, eine identifizierbare Handlung auszuführen (z.B. das Öffnen einer verschlossenen Tür).
2. Annäherung (z.B. mit der Hand) an die Koppelfläche eines Empfänger, damit Aufbau eine Wechselstromkreises; die Rückführung erfolgt über parasitäre Kapazitäten.
3. Empfänger „erkennt" die unregelmäßigen Pilottöne
4. Er erzeugt ein Belastungstelegramm durch Impedanz-Änderung der Eingangstufe in einem zufälligen jedoch sinnvollen Rhythmus.
5. Der Geber dekodiert aus dem Belastungstelegramm BT eine Handlungsanweisung
6. Damit verschlüsselt er seinen Identifizierungsdaten, und wählt z.B. eine Übertragungsfrequenz, Baudrate und Übertragungsverfahren aus (z.B. ASK, FSK usw.)
   (s. Abb. 6)
7. Der Geber gibt die verschlüsselten Signale aus und erzeugt anschließend wieder einen Pilotton

8. Der Empfänger verstärkt, dekodiert und entschlüsselt die Gebersignale
9. Bei Übereinstimmung einer bestimmten Codefolge wird ein Impuls ausgegeben, z.B. zum Öffnen eines Verschlussmechanismus (evtl. über ein Steuergerät).
10. Beim nächsten Pilotton gibt er dem Empfänger eine „OK"-Meldung und weitere Informationen über ein neues Belastungstelegramm. In dem Belastungstelegramm können Informationen enthalten sein, die vom Codegeber stammen oder durch diesen veranlasst wurden.
11. Wenn sich der Benutzer entfernt, bricht der Dialog ab. Der Geber generiert dann nur noch Pilottöne und der Empfänger meldet die Entfernung (z.B. Schließbefehl).
12. Zwischendurch „untersuchen" Geber und Empfänger ständig Ihre Umgebung nach Störungen.

Durch das unregelmäßige Ausgeben von Pilottönen sollen Kollisionen bei Verwendung mehrerer Geber weitgehend vermieden werden. Dabei soll der Abstand der Frequenzausgabe (burst) aus einem fixen und mindestens einem zufälligen Zeitanteil bestehen, der eine bestimmte Dauer nicht überschreiten darf (sog. dirty burst).

Beispiel einer Generierung von „dirty bursts" in der Programmiersprache „C", wobei angenommen wird, das der Geber seine Funktionen durch einen Microcontroller (oder eine vergleichbare Logik) erfüllt:

```
While(1)// Hauptschleife
{
A=50    // fester Burstanteil in ms
B=RND(50) // variabler Burstanteil wird duch Zufallsfunktion
              RND gebildet
Sleep(A+B)  // stromsparender Zustand (Burst)
Pilot(1)    // nach dem „Aufwachen" wird der Pilotton
              ausgesendet, und ein evtl. Belastungstelegramm
```

```
            geprüft
check_BT()
}
```

Weitere beispielhafte Anwendungen

Zusätzlich zu identifizierenden Informationen können von Sensoren erfasste Daten an den Empfänger übertragen werden. Etwa in der Medizintechnik ist es möglich, bioelektrische Daten (EEG,EMG,EKG usw.) sowie Puls, Temperatur(en), Atmung, Drücke (Blut, Schwellungen etc.) zu digitalisieren und im Geber z.B. zwischenzuspeichern (Logger). Bei Annäherung an einen Empfänger kann dieser über das BT z.B. Sensoren auswählen oder den Zwischenspeicher auslesen (flush). Der Geber kann als ein Art elektronisches Pflaster ausgelegt sein, welches auf eine zu untersuchende Körperstelle geklebt wird. Der Empfänger kann über sein Belastungstelegramm auch Stimulationen (z.B. elektr. Reize) auslösen. Eine Beeinträchtigung des Patienten mittels Funkwellen erfolgt nicht. Die Datenübertragung erfolgt über die Haut, nicht durch den Körper und dessen Zellen.

Elektrisch abfeuerbare Waffen können benutzerabhängig funktionieren (sog. Smartguns), wenn eine solche Waffe mit einem Empfänger ausgerüstet ist. Im Belastungstelegramm können auch Angaben über den Munitionsinhalt (z.B. durch Digitalisieren der Federspannung des Magazins) und die Gebrauchsfähigkeit enthalten sein. Die Waffe funktioniert nur, wenn der Benutzer einen autorisierenden Geber mit sich führt. und die Waffe in seinen eigenen Händen hält. Dies kann Unfällen (z.B. mit Kindern) oder Missbrauch vorbeugen.

Eine weitere sinnvolle Anwendung könnte die eines elektronischen Tickets sein. Dabei kann der Geber in einem

nicht flüchtigem Speicher Daten vorhalten, die Aufschluss über z.B. die Nutzung geben (Gültigkeit, Preisklasse, Sitzrang usw.). Beim Betreten einer gebührenpflichtigen Einrichtung (Kino, Theater, Sport- o. Freizeitstätte, öffentliche Verkehrsmittel etc.) können über das Belastungstelegramm eines am Eingang angebrachten Empfängers (z.B. mit Koppelfolie im Fußboden) Abbuchungen vorgenommen, Leitinformationen (z.B. Sitzplatz anzeigen usw.) gegeben, oder sonstige Informationen übertragen werden.

Das quasi unidirektionales Dialogsystem ist überall da komfortabler und kostengünstiger einsetzbar, wo bisher andere drahtlose Technologien (Funk, Transponder, IR-Licht usw.) Verwendung fanden, und die entweder auf einen Dialog verzichteten und/oder nur mit erheblichen Aufwand und/oder Sicherheitsrisiken realisiert werden konnten. Eine Verbindung der unterschiedlichen Technologien ist möglich, z.B. um diese sicherer oder komfortabler zu machen.

Durch eine einfach zu realisierende rhythmische Änderung der Eingangsimpedanz des Empfängers erhält der Geber Informationen. Dies ist so nur in einem Wechselstromkreis möglich, wie er vorzugsweise bei kapazitiver Datenübertragung entsteht. Ein Dialog kann stattfinden, weil der Geber mit seinem frequenten Pilotsignal den Träger für das Belastungstelegramm des Empfängers liefert, was prinzipiell eine Amplitudenmodulation darstellt. Bei konstantem Ausgabepegel wird der Pilotton nicht belastet, vielmehr ist die rhythmische Belastung im parasitären Rückführungskreis zu detektieren. Das wiederum erschwert das unbefugte Abhören des Belastungstelegramms BT.

Die Erfindung vereinfacht und verbilligt bidirektionale Datenübertragungssysteme und ermöglichen eine handlungsintegrierte Identifikation eines Benutzers. Damit

kann das System bevorzugt in „Personal Area Networks" (PAN) verwendet werden. Außerdem kann es bestehende Technologien um Komfort und/oder Sicherheitsfaktoren ergänzen.

PATENTANSPRÜCHE

1. Verfahren zur Abwicklung eines Datentransfers zwischen einem Mastersystem (Geber) und einem Slavesystem (Empfänger) bei welchem seitens des Mastersystems ein Signalereignis in einen Empfangsbereich des Slavesystems hinein abgegeben wird und
die Empfangsaufnahmeeigenschaften des Slavseystems definiert moduliert und
seitens des Mastersystems erkannt und ausgewertet werden.

2. Verfahren nach Anspruch 1, wobei der Datentransfer auf Grundlage kapazitiver Wechselwirkungseffekte abgewickelt wird.

3. Verfahrne nach Anspruch 1 oder 2, wobei seitens des Mastersystems eine Pilotsequenz emittiert wird und während des Eingangs der Pilotsequenz die Eingangsimpedanz des Slavesystems nach Maßgabe eines Datenmusters moduliert wird.

4. Verfahren nach wenigstens einem der Ansprüche 1 bis 3, wobei seitens des Mastersystems die modulierte Änderung der Eingangsimpedanz des Slavesystems erfasst wird.

5. Verfahren nach wenigstens einem der Ansprüche 1 bis 4, wobei aus dem seitens des Mastersystems erfassten Modulationsmuster der Eingangsimpedanz des Slavesystems ein Datensatz generiert wird und dieser Datensatz maßgeblich ist für den Informationsinhalt oder für die Zulässigkeit einer Fortsetzung des Datentransfer von dem Mastersystem zu dem Slavesystem.

6. Verfahren nach wenigstens einem der Ansprüche 1 bis 5, wobei im Bereich des Mastersystems aus den, aus dem Aufnahmeverhalten des Slavesystems gewonnenen Signalen Daten gewonnen werden auf deren Grundlage eine Verschlüsselung der seitens des Slavesystems weiter ausgesendeten Daten erfolgt.
7. dass im Bereich des Slavesystems bei der Generierung des für die Modulation der Eingangsimpedanz relevanten Datenmuster ein Zeitwert berücksichtigt wird.

7. Verfahren nach wenigstens einem der Ansprüche 1 bis 6, wobei im Bereich des Slavesystems für die Modulation der Eingangsimpedanz Informationsinhalte der seitens des Mastersystems generierten Signale berücksichtigt werden.

8. Verfahren nach wenigstens einem der Ansprüche 1 bis 7, wobei die Modulation der Eingangsimpedanz des Slavesystems unter Rückgriffnahme auf eine Verschlüsselungsprozedur erfolgt.

9. Verfahren nach wenigstens einem der Ansprüche 1 bis 8, wobei die seitens des Slavesystems zur Bereitstellung der für die Modulation der Eingangsimpedanz maßgeblichen Datenmuster beigezogene Verschlüsselungsprozedur auf Grundlage von Informationsinhalten der seitens des Mastersystem ausgegebenen Signalsequenz konfiguriert oder beeinflusst wird.

10. Verfahren nach wenigstens einem der Ansprüche 1 bis 9, wobei im Rahmen der Dialogaufnahme eine Kongruenzanalyse zunächst auf Grundlage eines niedrigen Verschlüsselungsniveaus erfolgt, und dass das Verschlüsselungsniveau anschließend angehoben wird.

11. Verfahren nach wenigstens einem der Ansprüche 1 bis 10, wobei die für das angehobene Verschlüsselungsniveau

maßgeblichen Informationsinhalte zumindest zunächst auf niedrigerem Verschlüsselungsniveau transportiert werden.

12. Verfahren nach wenigstens einem der Ansprüche 1 bis 11, wobei über das Mastersystem eine, als Autorisierungskennung gewertete Signalsequenz selektiv abgebbar ist.

13. Verfahren nach wenigstens einem der Ansprüche 1 bis 12, wobei über das durch Impedanzmodulation zurückgeführte Signal des Slavesystems eine Konfigurationsänderung des Mastersystems abwickelbar ist.

14. Verfahren nach wenigstens einem der Ansprüche 1 bis 13, wobei der Datentransfer zwischen dem Mastersystem und dem Slavesystem zur Abwicklung eines Zahl, Buchungs-, Wertstellungs- oder Zugangsnachweisvorganges herangezogen wird.

15. Verfahren nach wenigstens einem der Ansprüche 1 bis 14, wobei der Datentransfer zwischen dem Mastersystem und dem Slavesystem zur Abwicklung eines Vorganges zur Änderung des Verriegelungszustandes eines Kraftfahrzeuges herangezogen wird.

16. Verfahren nach wenigstens einem der Ansprüche 1 bis 15, wobei der Datentransfer zwischen dem Mastersystem und dem Slavesystem zur Funktionsfreigabe von Gerätschaften herangezogen wird.

17. Verfahren nach wenigstens einem der Ansprüche 1 bis 16, wobei der Datentransfer zwischen dem Mastersystem und dem Slavesystem zur Durchführung einer Präsenzanalyse herangezogen wird.

18. System zur Abwicklung eines Datentransfers mit:

einer einem Mastersystemkomponente (Geber) und
einer Slavesystemkomponente (Empfänger)
wobei die Mastersystemkomponente derart ausgebildet ist, dass diese geeignet ist, ein Signalereignis in einen Empfangsbereich der Slavesystemkomponente hinein abzugeben, und
die Slavesystemkomponente derart ausgebildet ist, dass diese es ermöglicht, die Empfangsaufnahmeeigenschaften derselben definiert zu modulieren, wobei
im Bereich der Mastersystemkomponente Vorkehrungen getroffen sind, die Änderungen der Empfangseigenschaften der Slavesystemkomponente zu Erfassen und basierend auf dieser Erfassung den weiteren Datentransfer zu bestimmen.

19. Mastersystemkomponente für ein System nach Anspruch 18, wobei diese eine Signalausgabeeinrichtung aufweist die als Flächenelektrode ausgebildet ist.

20. Mastersystemkomponente nach Anspruch 19, wobei diese eine elektronische Signalverarbeitungseinrichtung umfasst.

21. Mastersystemkomponente nach Anspruch 20, wobei die Signalverarbeitungseinrichtung Zugriff zu einer Schlüsseldatenspeichereinrichtung hat.

22. Mastersystemkomponente nach wenigstens einem der Ansprüche 9 bis 21, wobei diese in einem scheckkartenförmigen Grundkörper aufgenommen ist.

23. Mastersystemkomponente nach wenigstens einem der Ansprüche 19 bis 22, wobei diese Teil eines Fahrzeugschlüsselsystems bildet.

24. Slavesystemkomponente für ein System nach Anspruch 18, wobei diese eine Empfangseinrichtung aufweist, zum Empfang

von Eingangsereignissen auf Grundlage kapazitiver Wechselwirkungseffekte.

25. Slavesystemkomponente wobei die Empfangseinrichtung im Bereich eines Kassensystems, eines Personendurchgangsbereiches, eines Verkaufssystems oder einer Gerätschaft angeordnet ist.

26. Slavesystemkomponente nach Anspruch 24, wobei diese Teil eines Fahrzeugtürverriegelungssystems bildet.

27. Verfahren zur Änderung des Verriegelungszustandes eines Kraftfahrzeuges unter Abwicklung eines Datentransfers zwischen einem Mastersystem (Geber/Schlüssel) und einem Slavesystem (Empfänger/fahrzeugseitige Schaltungskomponente) bei welchem seitens des Mastersystems ein Signalereignis in einen Empfangsbereich des Slavesystems hinein abgegeben wird und
die Empfangsaufnahmeeigenschaften des Slavseystems definiert moduliert und
seitens des Mastersystems erkannt und ausgewertet werden.

28. Verfahren zur Änderung des Verriegelungszustandes eines Kraftfahrzeuges unter Abwicklung eines Datentransfers zwischen einem Mastersystem (Schlüsseleinrichtung) und einem Slavesystem (fahrzeugseitige Schaltungskomponente) insbesondere nach Anspruch 27, bei welchem seitens des Slavesystems ein Signalereignis in einen Empfangsbereich des Mastersystems hinein abgegeben wird und
die Empfangsaufnahmeeigenschaften des Mastersystems definiert moduliert und
seitens des Slavesystems erkannt und ausgewertet werden

Verfahren nach Anspruch 27 oder 28 wobei der Datentransfer auf Grundlage kapazitiver Wechselwirkungseffekte abgewickelt wird.

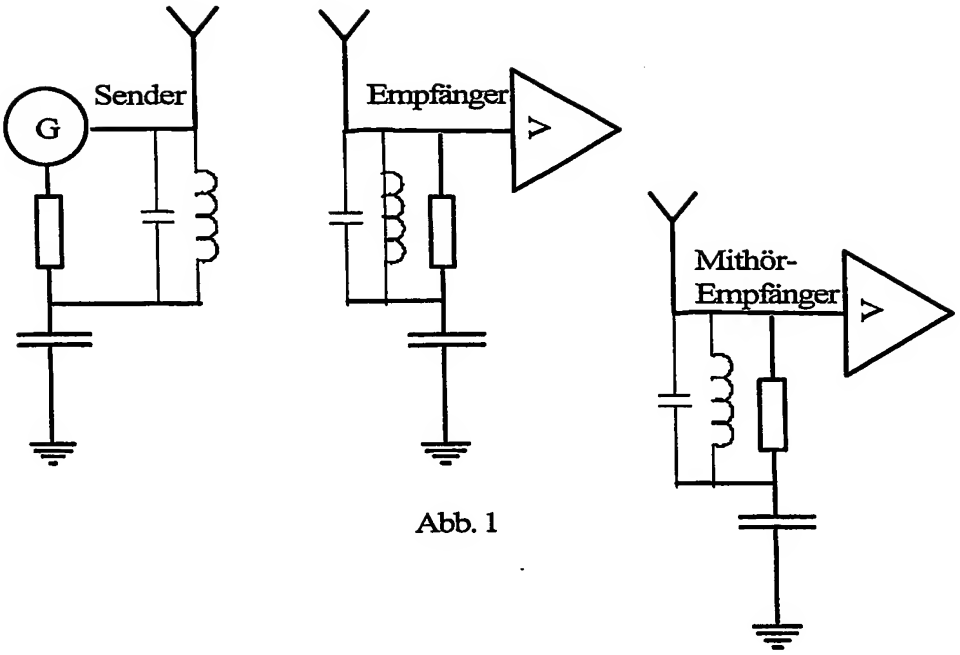

Abb. 1

5

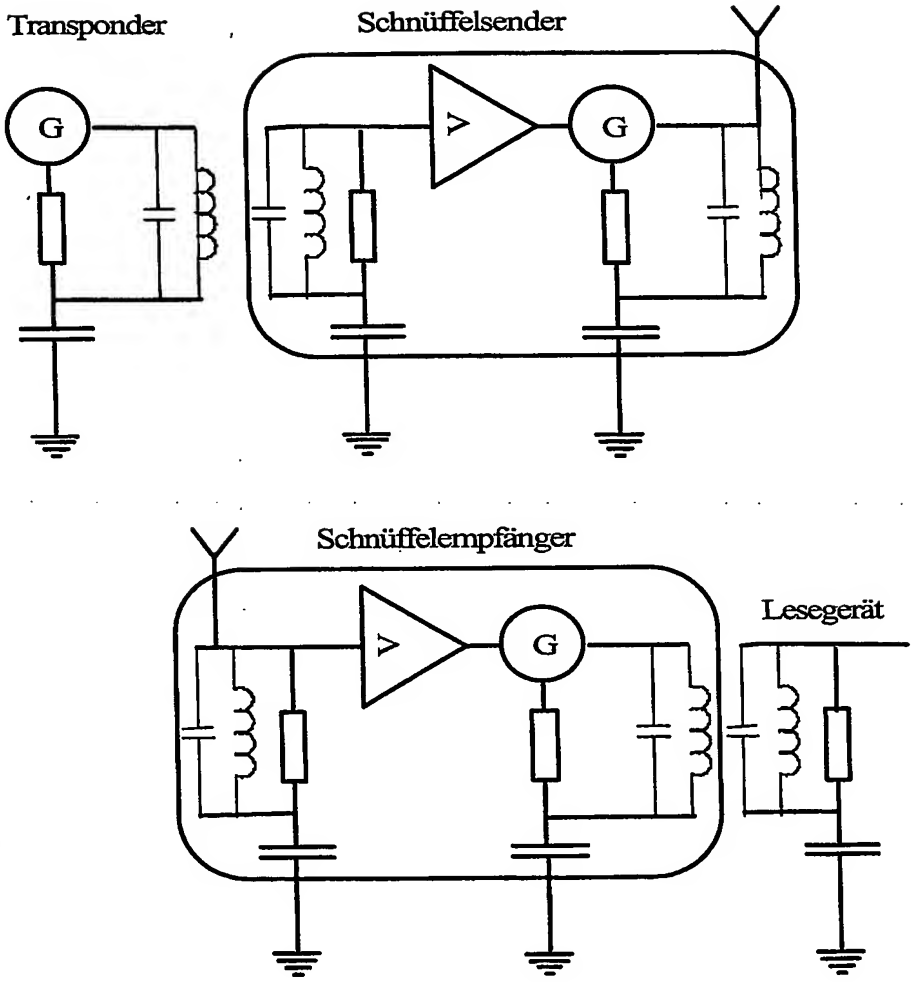

Abb. 2 Reichweitenüberbrückung mittels sog. "Schnüffler"

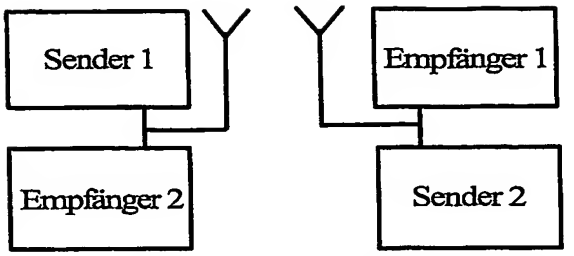

Abb. 3 Challenge/Response-System

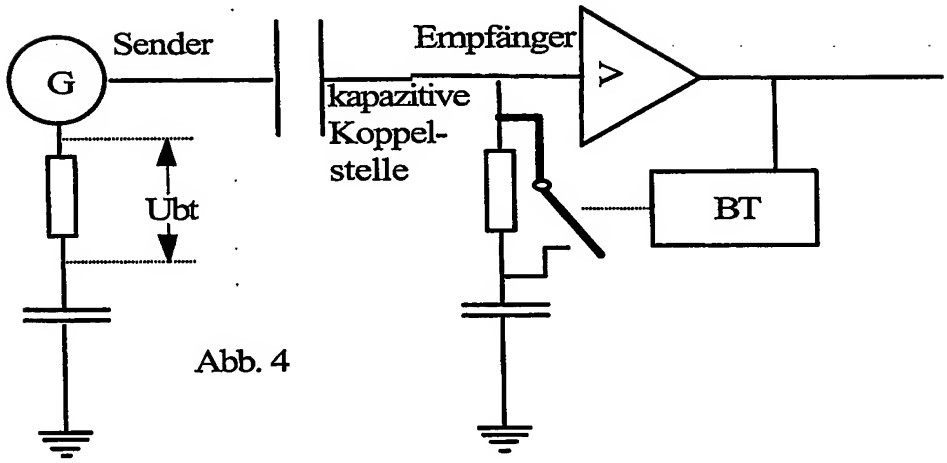

Abb. 4

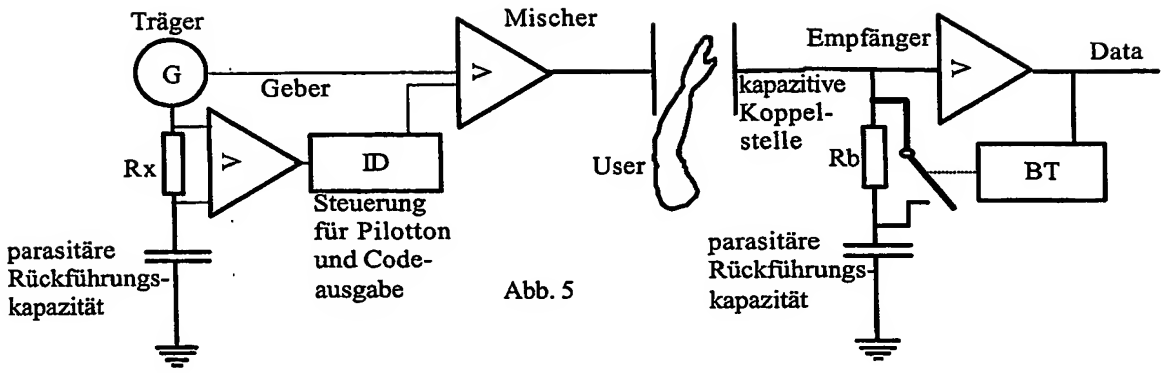
Träger
G
Geber
Mischer
Empfänger
Data
kapazitive
Koppel-
stelle
Rx
ID
Steuerung
für Pilotton
und Code-
ausgabe
User
Rb
BT
parasitäre
Rückführungs-
kapazität
parasitäre
Rückführungs-
kapazität

Abb. 5

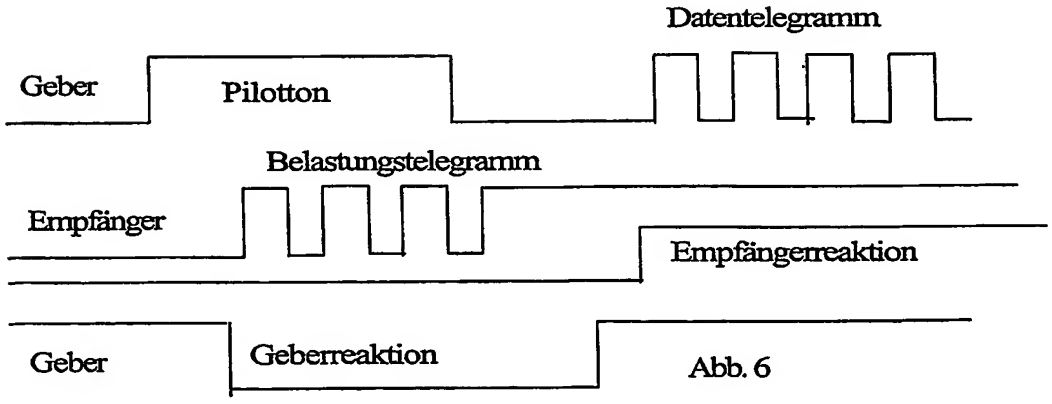
Datentelegramm
Geber
Pilotton
Belastungstelegramm
Empfänger
Empfängerreaktion
Geber
Geberreaktion

Abb. 6